

J. W. Price, 944/261.8433

Noboru Kattamelal

S.N. 09/593,677

日本国特許庁

PATENT OFFICE

JAPANESE GOVERNMENT AKA1-BL38



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日  
Date of Application:

1999年 6月15日

出願番号  
Application Number:

平成11年特許願第167899号

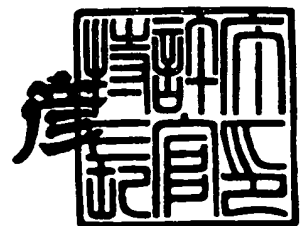
出願人  
Applicant(s):

松下電器産業株式会社

2000年 6月 2日

特許庁長官  
Commissioner,  
Patent Office

近藤隆彦



出証番号 出証特2000-3041224

【書類名】 特許願

【整理番号】 2022510291

【提出日】 平成11年 6月15日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/00

【発明者】

    【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

    【氏名】 勝田 昇

【発明者】

    【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

    【氏名】 茨木 晋

【発明者】

    【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

    【氏名】 井上 信治

【発明者】

    【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

    【氏名】 館林 誠

【特許出願人】

    【識別番号】 000005821

    【氏名又は名称】 松下電器産業株式会社

【代理人】

    【識別番号】 100097445

    【弁理士】

    【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【プルーフの要否】 不要

【書類名】 明細書

【発明の名称】 暗号処理装置および暗号復号装置および暗号伝送方法および記録装置およびデータ書き込み装置

【特許請求の範囲】

【請求項 1】 暗号処理手段と複数の入力データ解析手段と前記入力データ読み取り手段を制御し暗号処理位置を検出して暗号処理手段に暗号処理させる制御手段を具備し、前記制御手段は、暗号処理手順を記述した暗号処理記述データを読み取り、前記暗号処理記述データに基づき暗号処理制御を行うことを特徴とする暗号処理装置。

【請求項 2】 暗号化処理記述データは、専用に定義された入力データ解析処理の組み合わせによる処理手順を含み、入力データ解析装置は、前記専用に定義された入力解析処理を行うことを特徴とする請求項 1 記載の暗号処理装置。

【請求項 3】 入力データ解析手段としてデータ中のデータヘッダー位置を検出するヘッダー検出手段を少なくとも具備することを特徴とする請求項 1 記載の暗号処理装置。

【請求項 4】 入力データ解析手段としてデータ中の読み取り基本単位 of データ長を検出するデータ長検出手段を少なくとも具備することを特徴とする請求項 1 記載の暗号化装置。

【請求項 5】 暗号復号処理手段と複数の入力データ解析手段と前記入力データ読み取り手段を制御し暗号処理位置を検出して暗号処理手段に暗号処理させる制御手段を具備し、前記制御手段は、暗号処理手順を記述した暗号処理記述データを読み取り、前記暗号処理記述データに基づき暗号復号処理制御を行うことを特徴とする暗号復号処理装置。

【請求項 6】 暗号化処理記述データは、専用に定義された入力データ解析処理の組み合わせによる処理手順を含み、入力データ解析装置は、前記専用に定義された入力解析処理を行うことを特徴とする請求項第 6 項記載の暗号復号処理装置。

【請求項 7】 入力データ解析手段としてデータ中のデータヘッダー位置を検出するヘッダー検出手段を少なくとも具備することを特徴とする請求項 5 記載

の暗号復号装置。

【請求項 8】入力データ解析手段としてデータ中の読み取り基本単位の詳細長を検出するデータ長検出手段を少なくとも具備することを特徴とする請求項 5 項記載の暗号復号装置。

【請求項 9】伝送データを暗号化鍵と暗号処理記述データに基づき暗号化し、前記暗号化により暗号化された暗号化データと暗号化鍵および暗号処理記述データを伝送することを特徴とする暗号伝送方法。

【請求項 10】記録対象のデータを前記データに施される暗号処理内容を示す暗号処理記述データと前記暗号化処理記述データに基づき暗号化したデータを記録する記録装置。

【請求項 11】さらに、あらかじめ暗号処理記述データ記憶手段を持ち、データ記録時に前記記憶するデータを記録する際に適切な暗号処理記述データを送信することを特徴とする請求項 10 記載の記録装置。

【請求項 12】暗号化処理手段、記録装置内の暗号処理記述データ読み出し手段を具備し、データ書き込み時に、記録装置にある暗号化記述データを読み出し、それに基づき書き込みデータを暗号化して記録装置に書き込むことを特徴とするデータ書き込み装置。

【請求項 13】暗号処理記述データ読み取り手段と暗号復号化手段を持ち、データ読み出し時、それに対応する暗号処理記述データを読み出し、前記暗号処理記述手段に基づき読み出しデータを暗号復号化処理することを特徴とするデータ読み出し装置。

【請求項 14】暗号処理手段と暗号復号処理手段を持ち、暗号復号手段は、暗号化されたデータの暗号処理記述データを読みとり、それに基づき暗号復号処理し、暗号処理手段は、所望の暗号化処理を記述した第2の暗号化処理記述データを読み込み、読み込んだ第2の暗号処理記述データに基づき暗号化処理することを特徴とする暗号変換装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、データの伝送および蓄積においてデータを暗号化する暗号処理装置および暗号復号装置およびそれを用いた暗号伝送方法および暗号化処理して記録する記録装置およびデータ書き込み装置およびデータ読み出し装置および暗号変換装置に関するものである。

#### 【 0 0 0 2 】

##### 【従来の技術】

従来の暗号化処理は、データの伝送および蓄積等において許可のあるものだけがそれを利用できるようにするため用いられている。たとえば、テレビのデジタル放送においては、有料放送を行う際、番組データに暗号処理を施している。その際、暗号化処理するデータとしては、各伝送パケット内のデータのペイロード部分にのみ暗号化することが規定されている。したがって、送信側で規定された暗号アルゴリズムを用いて、規定された位置を暗号化する。一方、復号側は、規定された暗号復号アルゴリズムにより規定された領域を暗号復号処理すれば、元のデータを得る事が出来る。ここでの暗号復号アルゴリズムとは、たとえば、64ビットのブロック暗号としてDES暗号やFEAL暗号などの共通鍵暗号アルゴリズムあるいは、公開鍵暗号のRSA暗号といったものを指す。

#### 【 0 0 0 3 】

このように、従来の暗号装置では、暗号アルゴリズムを決定するのに加えて暗号処理する位置について正確に規定することで暗号化復号化処理をおこなっていた。

#### 【 0 0 0 4 】

##### 【発明が解決しようとする課題】

しかしながら、前記従来の暗号化処理では、暗号アルゴリズムに加えて、厳密にデータ中のどの領域を暗号化対象にするかを規定しているため、想定したデータ以外を暗号化復号化処理することが困難であった。

#### 【 0 0 0 5 】

たとえば、映像や音楽データなどを暗号化して記録する場合、それぞれを再生する場合にランダムアクセスによる再生や早送り、途切れのない再生などを行うため、各データの記録フォーマットにある基本アクセス単位で暗号化処理を切り

換えることが望まれている。

【0006】

また、すべてのデータをCBCモード（サイファースブロックチェーンモード）など最初のデータに依存して暗号化すると途中のデータをアクセスする場合も最初のデータから順に再生しなければならず不便である。

【0007】

したがって、暗号化するデータのフォーマットに応じてランダムアクセスに必要な情報は残して暗号化するといった暗号化領域や処理の更新タイミング等をそれぞれのシステムに応じて規定する必要がある。ところが、DVD-RAMディスクやハードディスクおよび固体メモリーカードなど大容量のメモリなどさまざまなフォーマットの映像や音声を記録することが想定される機器においては、それらのデータのコンテンツに応じて別々の暗号処理装置が必要になる問題があった。

【0008】

また、同一フォーマットであっても記録するメディアによってアクセス可能なデータ単位があり、記録メディアに依存したアクセス単位でアクセスが可能になるように暗号処理の更新位置を切り換える必要があるが、それぞれの記録メディア毎に暗号処理装置を用意することは、非常に効率が悪い問題があった。

【0009】

また、伝送路についてもその伝送パケット長などに依存して暗号処理領域を決定することが多く、複数の伝走路から受信する場合を考えるとそれぞれについて専用の暗号装置を持つのは、非効率的である。

【0010】

またに、デジタルデータ、蓄積メディアおよび伝送路のフォーマットについても今後更に新しいものが出現されてくることが考えらる。したがって、単にビット列を解読困難にするように設計された暗号アルゴリズムを、暗号化するデータ中の所望の位置に適切に施して行える暗号装置が必要とされていた。

【0011】

以上のような問題点を鑑み本発明は、データのフォーマット、記録されるメディアフォーマット、伝送路フォーマット等に応じた最適な暗号処理が特にそのフ

フォーマット専用により込むことなく行え、さらに今後出現するフォーマットについてもそれに適した暗号処理が可能な汎用的な暗号処理装置およびそれを用いた伝送方法および記録装置およびデータ書き込み装置およびデータ読み出し装置および暗号変換装置を提供することを目的とする。

【0012】

【課題を解決するための手段】

前記課題を解決するために本発明は、暗号処理手段と複数の入力データ解析手段と前記入力データ読み取り手段を制御し、暗号処理位置を検出して暗号処理手段に暗号処理させる制御手段を具備し、前記制御手段は、暗号処理手順を記述した暗号処理記述データを読み取り、前記暗号処理記述データに基づき暗号処理制御を行う構成であり、暗号処理記述データを入力することにより多様なデータフォーマットに大要可能な暗号処理装置とできる。

【0013】

また、本発明は、暗号処理記述データは、専用に定義された入力データ解析処理の組み合わせによる処理手順を含み、入力データ解析装置は、前記専用に定義された入力解析処理を行うものであり、暗号記述が効率的に行える。

【0014】

また、本発明は、入力データ解析手段としてデータ中のデータヘッダー位置を検出するヘッダー検出手段を少なくとも具備する構成である。

【0015】

また、入力データ解析手段としてデータ中の読み取り基本単位のデータ長を検出するデータ長検出手段を少なくとも具備する構成である。

【0016】

また、本発明は、暗号復号処理手段と複数の入力データ解析手段と前記入力データ読み取り手段を制御し、暗号処理位置を検出して暗号処理手段に暗号処理させる制御手段を具備し、前記制御手段は、暗号処理手順を記述した暗号処理記述データを読み取り、前記暗号処理記述データに基づき暗号復号処理制御を行う暗号復号処理装置の構成である。

【0017】



また、暗号化処理記述データは、専用に定義された入力データ解析処理の組み合わせによる処理手順を含み、入力データ解析装置は、前記専用に定義された入力解析処理を行う暗号復号装置の構成である。

## 【0018】

また、さらに本発明は、入力データ解析手段としてデータ中のデータヘッダー位置を検出するヘッダー検出手段を少なくとも具備する暗号復号装置の構成である。

## 【0019】

また、さらに入力データ解析手段としてデータ中の読み取り基本単位の詳細長を検出するデータ長検出手段を少なくとも具備する暗号復号装置の構成である。

## 【0020】

また、本発明は、伝送データを暗号化鍵と暗号処理記述データに基づき暗号化し、前記暗号化により暗号化された暗号化データと暗号化鍵および暗号処理記述データを伝送する暗号伝送方法である。

## 【0021】

また、本発明は、記録対象のデータを前記データに施される暗号処理内容を示す暗号処理記述データと前記暗号化処理記述データに基づき暗号化したデータを記録する記録装置の構成である。

## 【0022】

また、本発明は、あらかじめ暗号処理記述データ記憶手段を持ち、データ記録時に前記記憶するデータを記録する際に適切な暗号処理記述データを送信する記録装置の構成である。

## 【0023】

また、本発明は、暗号化処理手段、記録装置内の暗号処理記述データ読み出し手段を具備し、データ書き込み時に、記録装置にある暗号化記述データを読み出し、それに基づき書き込みデータを暗号化して記録装置に書き込むデータ書き込み装置の構成である。

## 【0024】

また、本発明は、暗号処理記述データ読み取り手段と暗号復号化手段を持ち、データ読み出し時、それに対応する暗号処理記述データを読み出し、前記暗号処理記述手段に基づき読み出しデータを暗号復号化処理するデータ読み出し装置の構成である。

## 【 0 0 2 5 】

また、本発明は、暗号処理手段と暗号復号処理手段を持ち、暗号復号手段は、暗号化されたデータの暗号処理記述データを読みとり、それに基づき暗号復号処理し、暗号処理手段は、所望の暗号化処理を記述した第2の暗号化処理記述データを読み込み、読み込んだ第2の暗号処理記述データに基づき暗号化処理する暗号変換装置の構成である。

## 【 0 0 2 6 】

## 【発明の実施の形態】

以下、本発明の実施の形態について図 1 から図 1 0 を用いて説明する。

## 【 0 0 2 7 】

## (実施の形態 1)

図 1 は、本発明の第 1 の実施の形態における暗号処理装置の構成図である。同図において、1 0 1 は、暗号処理装置、1 0 2 は、制御部、1 0 3 は、暗号処理部、1 0 4 は、フレーム長検出部、1 0 5 は、ヘッダー検出部である。以上の構成において以下その動作を説明する。

## 【 0 0 2 8 】

暗号処理装置 1 0 1 は、暗号化鍵と暗号処理記述情報に基づき入力データを暗号化処理する。暗号化鍵は、制御部 1 0 2 に入力されると暗号化処理部 1 0 3 に入力される。

## 【 0 0 2 9 】

暗号処理記述情報は、入力データ中のどの部分に暗号化するのかを示す情報、あるいは、どのようにその特定のデータ領域を見つけて暗号化処理するかという動作を表現した情報である。図 2 は、暗号処理記述情報を表現するために定義した処理命令関数の説明図である。同図において、4 つの専用命令関数を定義している。図 2 ( 1 ) の関数は、デジタルデータにおける読み出しの同期をとるこ

とが可能にするための同期信号パターンを検出するヘッダー検出関数である。これは、検出するヘッダーの検出パターンのビット数とそのパターンと検出開始位置を入力パラメータとして、入力データ中の検出開始位置から最初に検出される検出パターン位置へ参照位置を移動する処理であり、図 1 におけるヘッダー検出部 1 0 5 の処理を記述する。図 2 (2) は、同期パターンに囲まれた入力データのフレーム長を検出するフレーム長検出処理を示す関数である。これは、入力データが可変長である場合、よくそのフレーム長を示すコードが付加されている場合があり、それを検出する処理である。ヘッダーの先頭からそのコードが出現する位置のビット位置とそのコードの符号長、および表現されている値の単位がバイト単位かビット単位かを示す値を引数として検出した値に単位ビット倍されて、符号長が検出され、frame#length 値に値をいれる。これは、図 1 のフレーム長検出処理部 1 0 4 の処理を表現する。

【0 0 3 0】

図 2 (3) は、入力データ中の参照位置を引数分だけ移動させる処理である。

【0 0 3 1】

図 2 (4) は、暗号処理を示す関数で図 1 の暗号処理部 1 0 3 の処理を表現する。アルゴリズム番号は、DES や FEAL といったあらかじめ標準で準備した暗号アルゴリズムである。モードは、暗号の適応モード、block#length は、処理ブロック長であり、たとえば、64 ビットのブロック暗号で ECB モードであれば、64 ビットである。終了処理位置は、暗号処理する領域の最終ビット位置であり、もし暗号処理領域のビット数が処理ブロック長で割り切れなかったら終了処理位置を越えない最大の回数だけ処理するものとする。

【0 0 3 2】

図 3 は、図 2 で定義された関数を用いて記述された暗号処理記述情報の例の説明図である。同図で記述された処理は、同期ヘッダーパターンが 12 ビットで 16 進数表現で FFF であり、ヘッダー先頭位置より 31 ビットめから 13 ビットにフレーム長コードがあるデータについてフレーム長コード以下を DES アルゴリズムで CBC モードで処理することを記述したものである。このデータは、たとえば、MPEG 2 あるいは MPEG 4 標準で規定されたオーディオデータの A

ACで圧縮されたデータのフォーマットにある。このようなオーディオデータを再生する用途として、ランダムアクセス等を行いたい場合は、所望のフレーム位置に参照位置を移動して再生処理をおこなう必要があり、フレーム位置が検出しやすいように同期パターンを暗号化せずに残すとともに次のフレームの先頭を暗号化後でもわかるようにフレーム長コードも暗号化せずに残す方が便利である。

#### 【0033】

図3に戻って、最初のヘッダー位置は、データの先頭にあるとして、参照位置を0ビットめにし、その後ヘッダー位置を検出し、フレーム長コードを検出し、次に参照位置をフレーム長コード位置の直後に移動する。検出したフレーム長に基づき、暗号処理終了位置を算出した後、暗号処理を行う。その後、暗号処理終了位置に参照位置を移動して、再びヘッダ検出処理から繰り返すことでヘッダーおよびフレーム長コードを残した領域を暗号化処理する記述となる。

#### 【0034】

以上のように記述された情報をそのままテキスト形式でもよいし、あるいは、各関数命令および変数に適当な数値を割り当てることでデータ量の少ないバイトコードのプログラムとして暗号処理記述情報とする。以上のように記述された暗号記述情報が制御部102に入力される。

#### 【0035】

図1に戻って、制御部102は、暗号処理記述情報を解釈し、それに基づきヘッダー検出処理部105、フレーム長検出部104を制御し、暗号処理領域を検出するとともに、暗号処理タイミングになると暗号処理関数に示された処理に基づき暗号処理部103に暗号処理を行わせることにより暗号化データを得る。

#### 【0036】

以上のような動作により暗号処理装置101は、暗号処理記述情報に基づき所望の位置に暗号化処理できる。暗号処理記述情報は、図2のような命令関数のようにデジタルデータの多くのものに共通に存在するヘッダーやフレーム長コード検出命令を特別に持つことにより、簡潔な表現で大半のデジタルデータフォーマットについてヘッダー部分を残した部分への暗号化処理を記述できるし、もっと処理の簡単なフレーム単位に関係なく、一定長ごとに暗号処理することなど

多様な暗号処理を表現できる。

#### 【 0 0 3 7 】

(実施の形態 2)

図 4 は、本発明の第 2 の実施の形態である暗号復号装置の構成図である。同図において、4 0 1 は、暗号処理装置、4 0 2 は、制御部、4 0 3 は、暗号復号処理部、4 0 4 は、フレーム長検出部、4 0 5 は、ヘッダー検出部である。以上の構成において以下その動作を説明する。

#### 【 0 0 3 8 】

図 4 は、図 1 の暗号処理部 1 0 3 を暗号復号処理部 4 0 3 に置き換えたものである。

#### 【 0 0 3 9 】

暗号処理された位置については、まったく同様の処理によって導き出される。したがって、図 2 の命令関数に加えて decryption(algorithm#no, mode, blocklength, end#pnt) を図 2 の暗号処理を暗号復号処理に置き換えた形で定義してやれば、同様にその動作を記述できる。

#### 【 0 0 4 0 】

たとえば、図 3 の暗号化処理は、encryption 命令を decryption 命令に置き換えるだけで図 2 の記述に対する復号処理記述となる。したがって、あとは同様の処理により図 1 で暗号化されたデータは、復号処理される。

#### 【 0 0 4 1 】

図 5 は、図 1 と図 4 の暗号処理装置 1 0 1 と暗号復号処理装置 4 0 1 を用いた暗号伝送装置の構成図である。同図において、5 0 1 は、暗号処理記述情報、5 0 2 は、図 1 の暗号処理装置 1 0 1 と同等の処理を行う暗号処理装置、5 0 3 は、多重送信装置、5 0 4 は、受信多重分離装置、5 0 5 は、暗号処理記述言語 5 0 1 の暗号処理命令を暗号復号処理に置き換えた暗号処理記述情報、5 0 6 は、図 4 の暗号復号処理装置 4 0 1 相当の暗号復号処理装置である。以上の構成により、以下その動作を説明する。

#### 【 0 0 4 2 】

送信データは、暗号化処理装置 5 0 2 に入力される。暗号処理記述情報 5 0 1

は、図 3 で示したような暗号処理動作を記述したものであり、送信データを送信するのに適切な暗号処理を行うように記述する。たとえば、CBCモードを用いた場合伝送途中でエラーが発生すると再生が困難になることを考慮して、フレーム毎に処理を初期化して行うことなどで伝送エラーに対する対策を取るなどが考えられる。図 3 の記述もフレーム毎のCBC処理を行うことを記述している。

#### 【 0 0 4 3 】

図 5 に戻って、暗号処理装置は、暗号記述情報 5 0 1 と暗号化鍵 K を用いて送信データを暗号化処理して多重送信装置 5 0 3 に送られる。多重送信装置 5 0 3 は、暗号化された送信データに暗号化鍵 K と暗号処理記述情報 5 0 1 中の暗号処理命令部分を暗号復号処理命令に置き換えたものを多重して受信多重分離装置 5 0 4 へ伝送する。受信多重分離装置 5 0 4 は、暗号化鍵 K および暗号処理記述情報 5 0 5 を分離して暗号復号処理装置 5 0 6 に入力するとともに暗号化されてきたデータを暗号復号処理装置 5 0 6 へ入力する。暗号復号処理装置 5 0 6 は、暗号処理記述情報 5 0 5 に基づき、暗号復号処理することにより受信データを得る。以上のような動作により、暗号伝送装置自身は、送信するデータについて特別に作り込まれたものでなくても暗号処理記述情報により暗号化し、その暗号化処理情報を暗号化鍵とともに伝送することで送信データの特徴に応じて最適な暗号化処理を施して伝送できる。また、送信データの種類が 1 つではなく、映像情報やオーディオ情報など異なるフォーマットのデータが伝送される場合でも暗号処理記述情報を書き換えることで暗号処理装置を複数もつ必要がない。

#### 【 0 0 4 4 】

##### (実施の形態 3)

図 6 は、本発明の第 3 の実施の形態である暗号処理装置を用いたデータ書き込み読み出し装置およびデータ記憶装置の構成図である。同図において、6 0 1 は、データ書き込み読み出し装置、6 0 2 は、デジタルスチルカメラやオーディオプレイヤーなどに利用されるメモリカードに代表されるようなデータ記憶装置、6 0 3 は、制御部、6 0 4 は、鍵生成部、6 0 5 は、図 1 の暗号化処理装置の暗号処理部 1 0 3 に図 4 の暗号復号処理部 4 0 3 の機能をあわせて持たせた暗号／復号処理部、6 0 6 は、データ記憶装置 6 0 2 内の記憶するデータを格納した

り、データ記憶装置 6 0 2 からのデータ読み出し時にデータを格納する記録部、6 0 7 は、制御部、6 0 8 は、データ記憶装置 6 0 2 に記録される可能性があると思定されるいくつかのデータフォーマットに対してあらかじめ用意した暗号処理記述情報群を記録した暗号処理記述情報記憶部、6 0 9 は、データ記憶装置 6 0 2 に与えられたメディアID番号記憶部、6 1 0 は、データ記録部である。これは、近年、メモリーカードを用いたオーディオプレイヤーやカメラなどにおいて著作権の保護の対象となるデータのデジタル記録において複数のコピーが容易に作れない様に記録メディアのIDに依存したパラメータでデータを暗号化して記録することにより、著作権を守る処理を保証した製造者の装置だけが復号処理ができるようにすることで無数の複製を作られることを防止するためなどに用いることが出来る。以上のような構成について以下その動作を説明する。

#### 【0 0 4 5】

データ書き込み読み出し装置 6 0 1 は、たとえば、デジタルスチルカメラやオーディオプレイヤー内のメモリーカードとのインターフェイス部であったり、パーソナルコンピュータとメモリーカードを接続するインターフェイス部であったりするものであり、外部からの入力データをデータ記憶装置 6 0 2 に書き込んだり、逆に外部から指定によりデータ記憶装置 6 0 2 中のデータを読み出し出力することが想定される。ここでは、外部の入出力のかわりに記録部 6 0 6 からの書き込み、記録部 6 0 6 への読み出しにより説明する。

#### 【0 0 4 6】

データ記憶装置 6 0 2 への書き込み読み出し、制御部 6 0 3 および 6 0 7 間のデータ転送手順により行われる。

#### 【0 0 4 7】

図 8 は、データ書き込み時の制御部 6 0 3 と制御部 6 0 7 間の処理の説明図である。同図において、8 0 1 は、書き込みファイル指定処理、8 0 2 は、メディアIDおよび暗号処理記述情報送出处理、8 0 3 は、暗号化鍵設定処理、8 0 4 は、暗号処理記述情報設定処理、8 0 5 は、暗号化およびデータ送出处理、8 0 6 は、受信データ記録処理である。

#### 【0 0 4 8】

図8における左側の処理は、制御部603の処理であり、右側の処理は、制御部607の処理である。まず、制御部603は、書き込むファイル名を制御部802に送出する。制御部807は、指定されたファイル名につけられた拡張子（たとえば、そのデータのフォーマットの略称名をファイルの拡張子としてあらかじめ定義しておいたもの）を用いて、暗号処理記述情報記憶部608から送られてくるデータに対応した暗号処理記述情報を読み出し、メディアID番号記憶部605内のメディアIDとともに制御部603へ伝送する。制御部603は、メディアIDを鍵生成部604へ送る。鍵生成部604は、あらかじめ決められた処理に基づき暗号化鍵を生成し、暗号／復号処理部606へ暗号化鍵を入力する。次に、制御部603は、暗号記述情報を暗号／復号処理部605へ設定する。そして、記録部中の該当ファイルを暗号化処理部605へ送出し、暗号処理後のファイルを制御部607へ送出する。制御部607は受信データを指定ファイル名で記録する。

#### 【0049】

図9は、データ読み出し時の制御部603および制御部607の処理フローの説明図である。同図において、901は、読み出しファイル名送出处理、902は、暗号処理記述情報およびメディアID送出处理、903は、暗号化鍵設定処理、904は、暗号記述情報設定処理、905は、データ送信リクエスト処理、906は、データ送信処理、907は、データ受信処理である。

#### 【0050】

図9における左側の処理は、制御部603の処理、右側は、制御部607の処理である。まず、制御部603は、データ記憶装置602より読み出したファイル名を指定するためファイル名を制御部607へ送信する。制御部607は、指定ファイルの拡張子などの属性に基づいて、それに対応した暗号処理を復号するための暗号処理記述情報を選択し、メディアIDとともに制御部603に送信する。この時の暗号処理記述情報は、そのファイルが書き込まれた際の暗号処理記述情報の暗号処理命令部分を暗号復号処理命令に入れ替えたものと同じである。制御部603は、メディアIDを鍵生成部604へセットする。鍵生成部604は、データが書き込まれた時と同じ鍵を生成することになり、その鍵が暗号／復号



処理部 6 0 5 に設定される。次に制御部 6 0 3 は、暗号処理記述情報を暗号処理部へ設定する。その後、ファイルデータの送信を制御部 6 0 7 へリクエストする。制御部 6 0 7 は、リクエストを受け取ると指定されたファイルデータを制御部 6 0 3 へ送出する。制御部 6 0 3 は、受信したファイルデータを暗号／復号処理部 6 0 5 で復号処理させて記録部 6 0 6 へ記録する。

#### 【 0 0 5 1 】

以上の処理により、データ記憶装置 6 0 2 へは、そのデータフォーマットに適切な方法で暗号化処理され記録され、また、読み出し時には、正しく再生される。そして、データ書き込み読み出し装置 6 0 1 での処理手続きを踏まずに直接データにアクセスしてもデータは、データ記憶装置 6 0 2 のメディアIDに依存した暗号化されているため、複製を作っても正しく再生することが出来ず、不正な複製を防止出来る。

#### 【 0 0 5 2 】

図 7 は、データ記憶装置 6 0 2 内でのファイルの記録構成の説明図である。四角で囲まれたものがファイルとして管理されているものとする。データ記録装置 6 0 2 では、上段に示されたように各拡張子用にそれぞれ暗号処理記述情報が記憶されている。それは、最下段に示された各記録データファイルの拡張子によって関係づけて管理する。中段にある記録データファイルに対応した暗号鍵ファイルである。これは、先に説明した図 8、図 9 の手続きでは、存在しない。先の説明では、データ記憶装置 6 0 2 のデータは、同じ鍵で暗号化されることになるため、たとえば、図 7 の中段のように各ファイルに対応した暗号化鍵ファイルを生成させることで各ファイルに独立の鍵を持たせることができる。これは、たとえば、図 6 の鍵生成部が適当に乱数を生成し、それをメディア鍵とともにもう一つの鍵生成パラメータとして暗号化鍵を生成し、その乱数をそのファイル用暗号化鍵として制御部 6 0 3 を通じてデータ記憶装置 6 0 2 に伝送して暗号化鍵ファイルとして記憶させ、読み出し時には、メディアIDを送出する時に同時に暗号鍵ファイルをおくこととして、鍵生成部にメディアIDと暗号鍵ファイルを与えることにより暗号化鍵を生成させる。そうすることでデータ記憶装置 6 0 2 内のデータは、メディアIDとそのファイルに対応した暗号化鍵ファイルデータに依存した鍵

で暗号化されていることになり、各データは、別々の暗号化鍵で暗号化処理された形となりより解読に対して安全な管理が行える。また、想定されるフォーマットに対する暗号化処理記述情報をそのフォーマット毎に用意しているのですべてのファイル毎に暗号化処理記述情報ファイル持つ必要がなく、保存データ量を少なく出来る。

#### 【0053】

図10は、データを記録するメディアに適した暗号化処理に切り換える場合の暗号処理変換処理の説明図である。同図において1001、1002は、DVDやメモリカードなどの互いに異なる記録メディア、1003は、記録メディア1001のメディアID読み取り部、1004は、記録メディア1002のメディアID読み取り部、1005は、制御部、1006は、図2の暗号復号処理装置相当の暗号復号部、1007は、図1の暗号処理装置相当の暗号処理部である。同図の構成において、以下で暗号変換処理を説明する。

#### 【0054】

データを読み出しする場合にそのランダムアクセス性に影響するものとして、記録メディアのデータアクセス単位がある。すなわち、それぞれのメディアにおいて一度にアクセスできる単位で記録データのランダムアクセス単位が決まる場合がある。その際、暗号化処理もそのアクセス単位にあわせて処理単位を決定し、暗号化処理するれば、再生時のランダムアクセス性を悪化させることがない様にできる。そこで、各メディアにそれぞれそのアクセス単位に適合した暗号処理記述情報を持たせ、すべての記憶データファイルは、この記述に基づき暗号化して保存させる。図10は、記録メディア1001から記録メディア1002へデータを移し替える際の暗号変換処理を説明している。まずメディア鍵読み取り部1003および1004は、それぞれの記録メディア1001、記録メディア1002よりそれぞれのメディアIDを読み出してくる。制御部1005は、メディア鍵を暗号復号部1006、暗号処理部1007にそれぞれが接続された暗号処理に対応させて設定する。記録メディア1001では、各データは、記憶データの基本アクセス単位がたとえば512バイトなら、その単位で暗号化が行われるように記述した暗号化処理記述情報ファイルがあり、記録されているデータファイ

ルはこれに関係づけられている。ファイル送出時は、暗号処理記述情報を読み取り暗号復号処理部 1006 に設定した後、転送するデータを暗号復号処理部 1006 へ入力させる。記録メディア 1001 の場合と同様に記録メディア 1002 側にも記録メディアに適した暗号処理記述情報が用意されている。そして、データ受け入れ時は、制御部 1005 が記録メディア 1002 用の暗号処理記述情報を暗号処理部 1007 に設定する。そして、暗号復号処理部 1006 からの出力を暗号化処理部 1007 が暗号処理することで、記録メディア 1002 に適した暗号処理方法に変換された暗号化処理が施されて記録メディア 1002 に記録される。以上のような処理により、それぞれの記録メディアに適した暗号処理記述を暗号変換部にそれぞれ与えて、暗号復号処理、暗号処理を行うことでそれぞれのメディア内でのデータのアクセス操作性を失わせることのない暗号変換処理が行える。

#### 【0055】

以上、説明したように、本発明の実施の形態では、デジタルデータで一般に考えられるデータの同期ヘッダー検出およびフレーム長の検出といった処理を専用に規定した暗号記述言語に基づき暗号処理を記述した暗号処理記述情報と、専用に規定した処理を実現する処理部を具備し、それを制御する制御部が暗号処理記述情報を解釈して各処理を制御させる構成により、多様なデジタルフォーマットに対してその特性に応じた適切な暗号処理を行うことができる。

#### 【0056】

また、専用に規定した処理を定義したことにより、その記述が効率よく行えるとともに、暗号処理記述を実現する暗号処理装置も効率よく構成できる。そして、データを伝送する場合、暗号化鍵とともに暗号処理記述情報とともに送ることにより、伝送されるデータに特別に作り込んだ暗号復号装置を作ることなく多様なデジタルデータの暗号伝送を効率的な装置構成で実現することが出来る。

#### 【0057】

また、各デジタルフォーマットに対応した暗号処理記述情報をそれぞれ用意しておき、各ファイルは、その属性に応じて対応する暗号処理記述情報に関連付けることにより、個々に暗号化記述情報を管理する必要がなく、効率的な記録管

理が行える。また、各記録メディア毎に暗号記述情報により暗号化処理を規定しておき、データを移動する場合に、その記録メディアに適した暗号化処理に変換できるために、ランダムアクセス性などを失うことなく暗号データ記録が行える。

#### 【0058】

なお本実施の形態では、図2のように規定した特定の命令の規定に基づいて、たとえば、図3のようなプログラム記述を暗号処理記述情報としたが、それ以外でも、たとえば、同期検出ヘッダーパターンとフレーム長検出のためのパラメータを並べあげたパラメータ記述的な表現を用いてもよいし、C言語のような汎用なソフトウェア記述言語を用いてもよい。また、特別に規定した処理も、ヘッダー検出やフレーム以外のものでよい。たとえば、処理が複雑になるがヘッダーを検出してフレーム長を同時に検出処理を規定することでも出来し、逆にもう少し汎用的な定義として、指定ビット参照位置を移動して指定のビット数を読み取る命令を算術演算で表現する方法もある。また、記述されたプログラムもテキストのままでもよいし、所定の方法によりバイナリーコードへ変換して効率的に送ることも考えられる。

#### 【0059】

また、本実施の形態では、入力データ解析手段としてヘッダー検出部、フレーム長検出部を持っているが、特にそれだけに限定しているものではない。たとえば、暗号処理記述データの専用命令関数が単なる参照位置移動とデータ読み出しなどで記述されるときなどの時では、単にビットシフト部やデータ読み出し部などの単純な処理のものであってもよい。また、入力解析処理手段が入力データのみを見て動作しているものを実施例で示したが、たとえば動的に外部からフレーム長を受け取る場合など考えられる。これらについても暗号処理記述データとして外部からのパラメータ制御を規定し、入力解析手段として外部入力手段を処理部に持たせることでこれを行うことが出来る。

#### 【0060】

また、本実施の形態における暗号伝送装置における伝送方法についても暗号化鍵に加えて暗号処理記述情報が復号側に送られる構成であれば、さまざまな伝送方

法が考えられ特に本実施の形態の伝送方法に限定するものではない。

【0061】

また、本実施の形態においては、各データについて、そのフォーマット属性毎に暗号処理記述情報を用意してそれに各データを関連づけて管理した例を示したが、個々の独立に暗号処理記述情報を持ってもよいし、同じフォーマットでも別の暗号処理を行って別の暗号処理記述を持たせてもよい。同様に、記録メディア毎に暗号処理記述情報を持ち、それにより記録データの暗号化処理を規定した例を示したがここに暗号処理記述情報を持たせて別の暗号処理を行ってもよい。

【0062】

また、本実施の形態において、データの書き込み読み込み装置とデータ記憶装置に処理間の処理手続き例を示したが、その記録メディアの他のデータ伝送形式にあわせて伝送形態について特に限定するものでないし、最終的に書き込み時に用いた暗号化鍵と暗号処理記述情報が読み出し時に取得できて暗号復号出来ならば、別の方法でもよい。

【0063】

また、本実施の形態における暗号処理装置および暗号復号装置の構成以外でも同等の処理をソフトウェアですべて実現し、CPU上で実行するような構成でも一つのソフトウェアで多様なデータフォーマットに対応出来き、同様の効果が実現できる。

【0064】

また、本実施の形態では、暗号処理記述の例を図3に示したが、図2のような専用処理を組み合わせるとさまざまな処理が記述可能である。図11は、典型的なデジタルフォーマットでの暗号処理例の説明図である。固定長フレーム中のデータ領域への暗号処理や、可変長パケットの様にその長さを検出後、暗号処理領域を確定し、暗号化処理する。一定周期毎に処理を更新する場合など、これらの処理を図2に規定に基づき記述することも可能であり、多様な暗号処理を記述するために用いることが出来る。

【0065】

【発明の効果】

以上説明したように、本発明では、暗号処理をどの様に施すかを示す暗号処理記述情報をもとに暗号処理する暗号処理装置および暗号復号処理装置の構成により、多様なデジタルデータに対して適切な暗号処理を特にそのデータのために特別な装置を作ることなく、実現することが出来る。また、それを用いた効率的な暗号伝送装置が構成できる。また、メディア間で適切な暗号処理の付け替え変換が行える暗号変換装置、ファイル管理方法などを提供することができ、本発明の実用的効果は大きい。

【図面の簡単な説明】

【図 1】

本発明の第 1 の実施の形態における暗号処理装置の構成図

【図 2】

本発明の実施の形態における暗号処理記述情報を表現するために定義した処理命令関数の説明図

【図 3】

本発明の実施の形態における図 2 で定義された関数を用いて記述された暗号処理記述情報の例の説明図

【図 4】

本発明の第 2 の実施の形態である暗号復号装置の構成図

【図 5】

本発明の実施の形態における暗号伝送装置の構成図

【図 6】

本発明の第 3 の実施の形態である暗号処理装置を用いたデータ書き込み読み出し装置およびデータ記憶装置の構成図

【図 7】

本発明の実施の形態におけるデータ記憶装置 6 0 2 内でのファイルの記録構成の説明図

【図 8】

本発明の実施の形態におけるデータ書き込み時の制御部 6 0 3 と制御部 6 0 7 間の処理フローの説明図

【図 9】

本発明の実施の形態におけるデータ読み出し時の制御部 6 0 3 および制御部 6 0 7 の処理フローの説明図

【図 1 0】

本発明の実施の形態における暗号処理変換処理の説明図

【図 1 1】

典型的なデジタルフォーマットでの暗号処理例の説明図

【符号の説明】

- 1 0 1 暗号処理装置
- 1 0 2 制御部
- 1 0 3 暗号処理部
- 1 0 4 フレーム長検出部
- 1 0 5 ヘッダー検出部
- 4 0 1 暗号処理装置
- 4 0 2 制御部
- 4 0 3 暗号復号処理部
- 4 0 4 フレーム長検出部
- 4 0 5 ヘッダー検出部
- 5 0 1 暗号処理記述情報
- 5 0 2 暗号処理装置
- 5 0 3 多重送信装置
- 5 0 4 受信多重分離装置
- 5 0 5 暗号処理記述言語
- 5 0 1 暗号処理記述情報
- 5 0 6 暗号復号処理装置
- 6 0 1 データ書き込み読み出し装置
- 6 0 2 データ記憶装置
- 6 0 3 制御部
- 6 0 4 鍵生成部

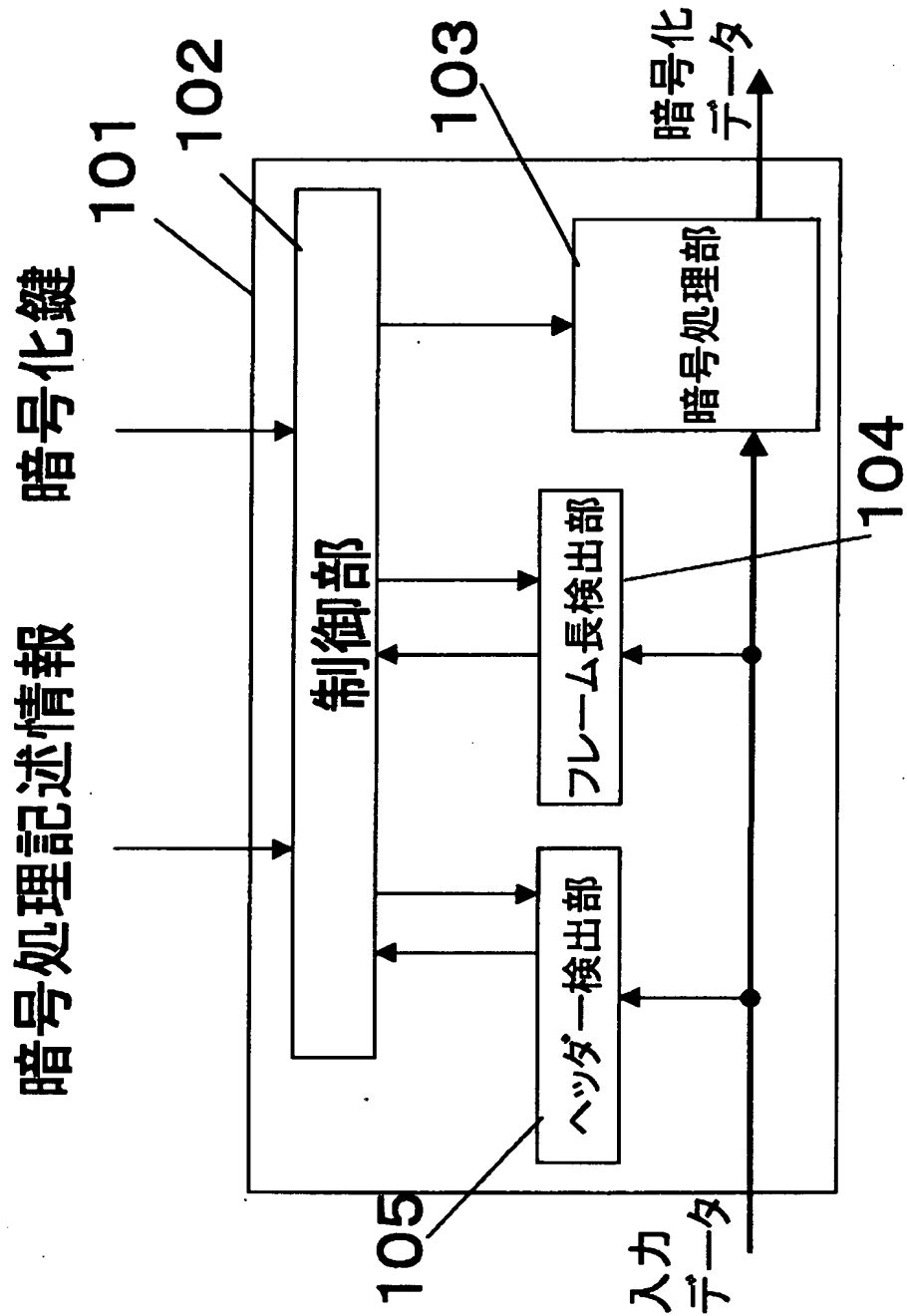
- 6 0 5 暗号／復号処理部
- 6 0 6 記録部
- 6 0 7 制御部
- 6 0 8 暗号処理記述情報記憶部
- 6 0 9 メディアID番号記憶部
- 6 1 0 データ記録部
- 8 0 1 書き込みファイル指定処理
- 8 0 2 メディアIDおよび暗号処理記述情報送出处理
- 8 0 3 暗号化鍵設定処理
- 8 0 4 暗号処理記述情報設定処理
- 8 0 5 暗号化およびデータ送出处理
- 8 0 6 受信データ記録処理
- 9 0 1 読み出しファイル名送出处理
- 9 0 2 暗号処理記述情報およびメディアID送出处理
- 9 0 3 暗号化鍵設定処理
- 9 0 4 暗号記述情報設定処理
- 9 0 5 データ送信リクエスト処理
- 9 0 6 データ送信処理
- 9 0 7 データ受信処理
- 1 0 0 1 記録メディア
- 1 0 0 2 記録メディア
- 1 0 0 3 メディアID読み取り部
- 1 0 0 4 メディアID読み取り部
- 1 0 0 5 制御部
- 1 0 0 6 図 2 の暗号復号処理装置相当の暗号復号部
- 1 0 0 7 図 1 の暗号処理装置相当の暗号処理部



【書類名】

図面

【図 1】



【図 2】

## (1) ヘッダー検出処理

head\_detect(detect\_pattern\_size, detect\_pattern, pnt\_offset)  
 detect\_pattern\_size: 検出ヘッダーのパターンビットサイズ  
 detect\_pattern: 検出するヘッダービットパターン  
 pnt\_offset: 検出処理の開始位置

ヘッダービットパターンを pnt\_offset 位置より検出を開始し、  
 最初のパターン検出位置へデータ参照位置 reference\_pnt を移動する。

## (2) フレーム長検出

frame\_length\_detect(length\_code\_position, lengthcode\_length, unit)  
 lengthcode\_position: ヘッダー検出位置からのフレーム長コードまでの位置  
 lengthcode\_length: フレームコード長を示すコードの長さ

unit: フレーム長コードが示す値の基本単位。ビットなら 1、バイトなら 8  
 参照位置から lengthcode\_position ビットだけ移動した位置から lengthcode\_length ビット  
 のデータを読み出し、unit 倍した値を frame\_length として算出。

## (3) 参照位置移動

reference\_position\_move(move\_no)  
 move\_no: 移動ビット数

## (4) 暗号処理

encryption(algorithm\_no, mode, blocklength, end\_pnt)  
 algorithm\_no: 暗号アルゴリズム番号 (1 は、DES、2 は FEAL など)  
 mode: 適応モード (1 は ECB、2 は OFB、3 は、CBC)  
 blocklength: 処理ブロック長  
 end\_pnt: 処理終了位置

現在の参照位置より指定の暗号処理を end\_pnt まで行う。処理ブロック長で  
 割り切れない場合は、end\_pnt を越えない回数行う。

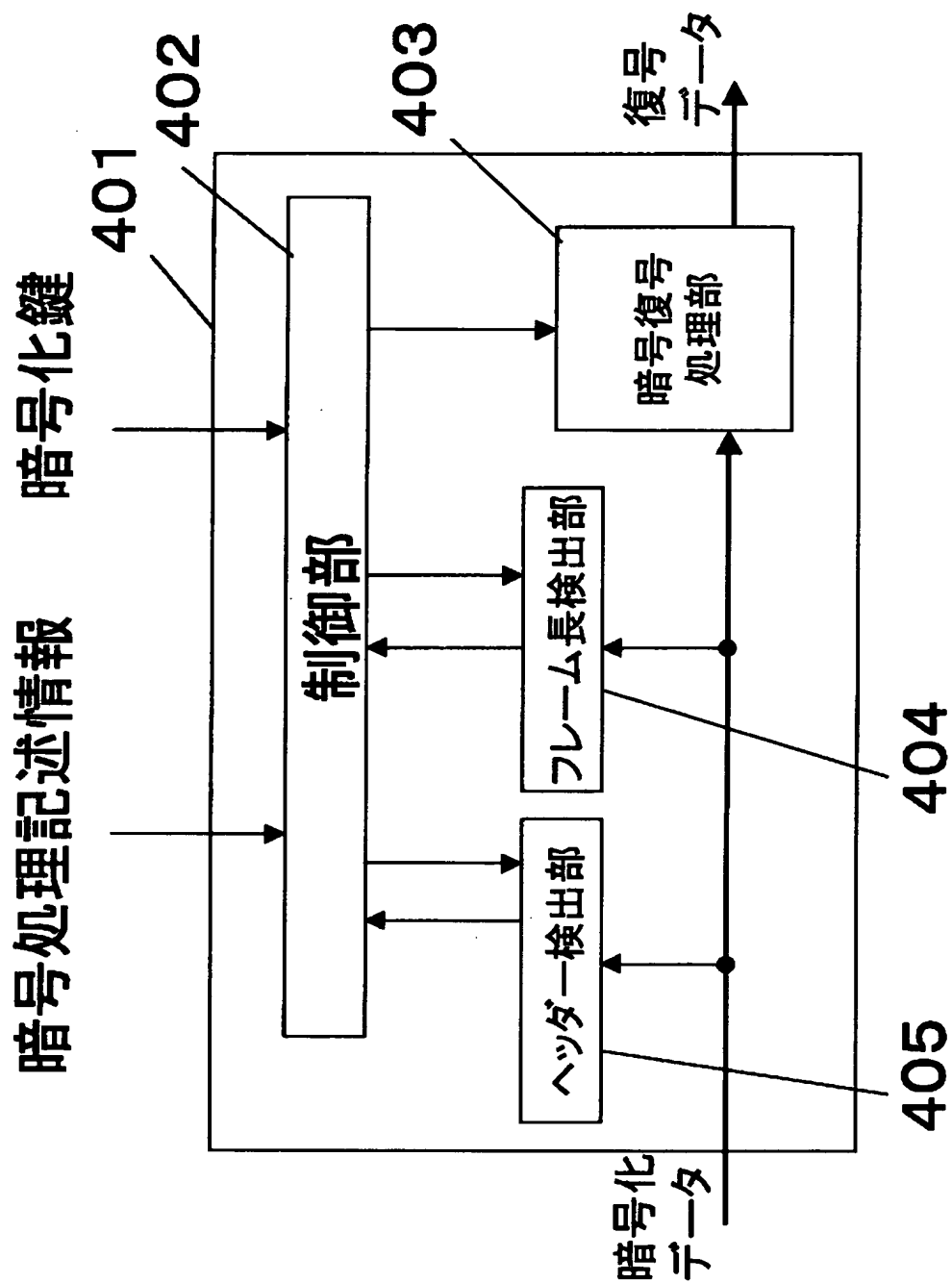
【図 3】

ヘッダーパターン: 12ビット、16進表示FFFF  
 フレーム長コード: ヘッダー先頭より31ビットめに13ビットでバイト単位表示  
 フレーム長コード以後フレーム終了までDESでCBCモード64ビット単位で暗号化する場合

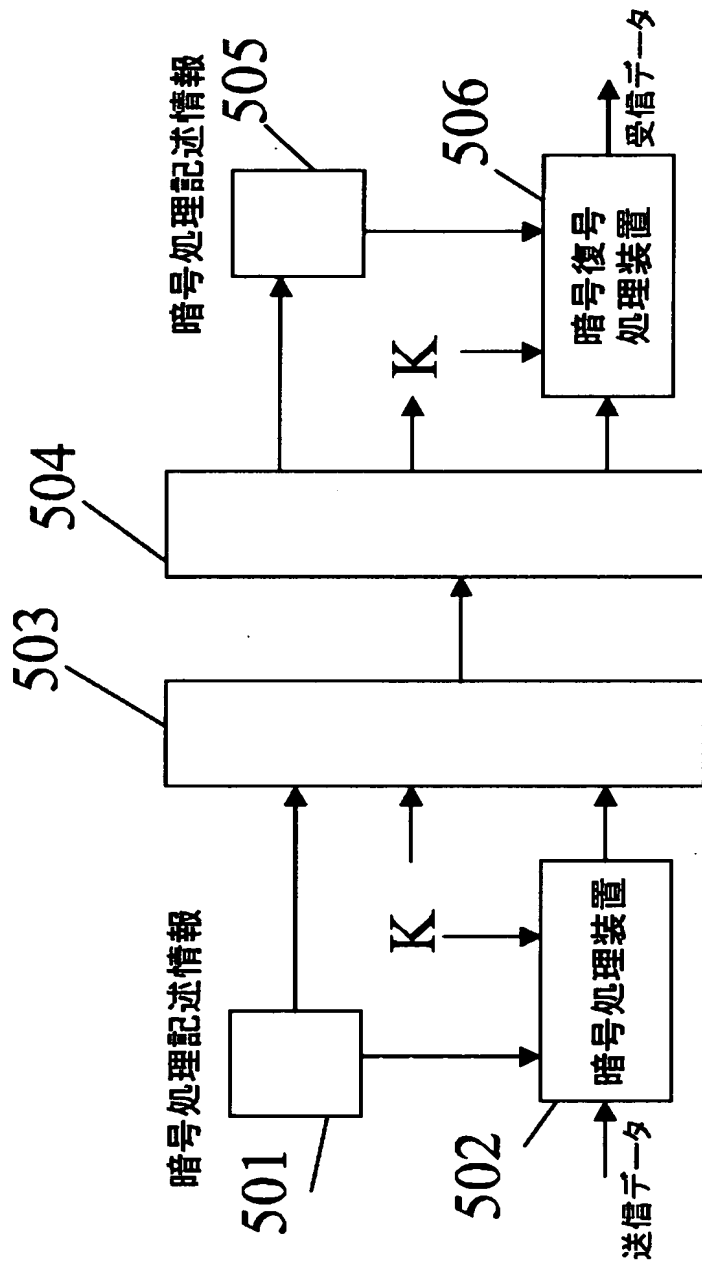
```

ref_pnt = 0;
while(endofdata)
{
    pnt_offset = ref_pnt;
    ref_pnt = head_detect(12, 0xffff, ref_pnt);
    frame_length = frame_length_detect(31, 13, 8);
    ref_pnt = reference_position_move(13);
    end_pnt = pnt_offset + framelength;
    encryption(1, 3, 64, end_pnt);
    ref_pnt = end_pnt;
}
end
    
```

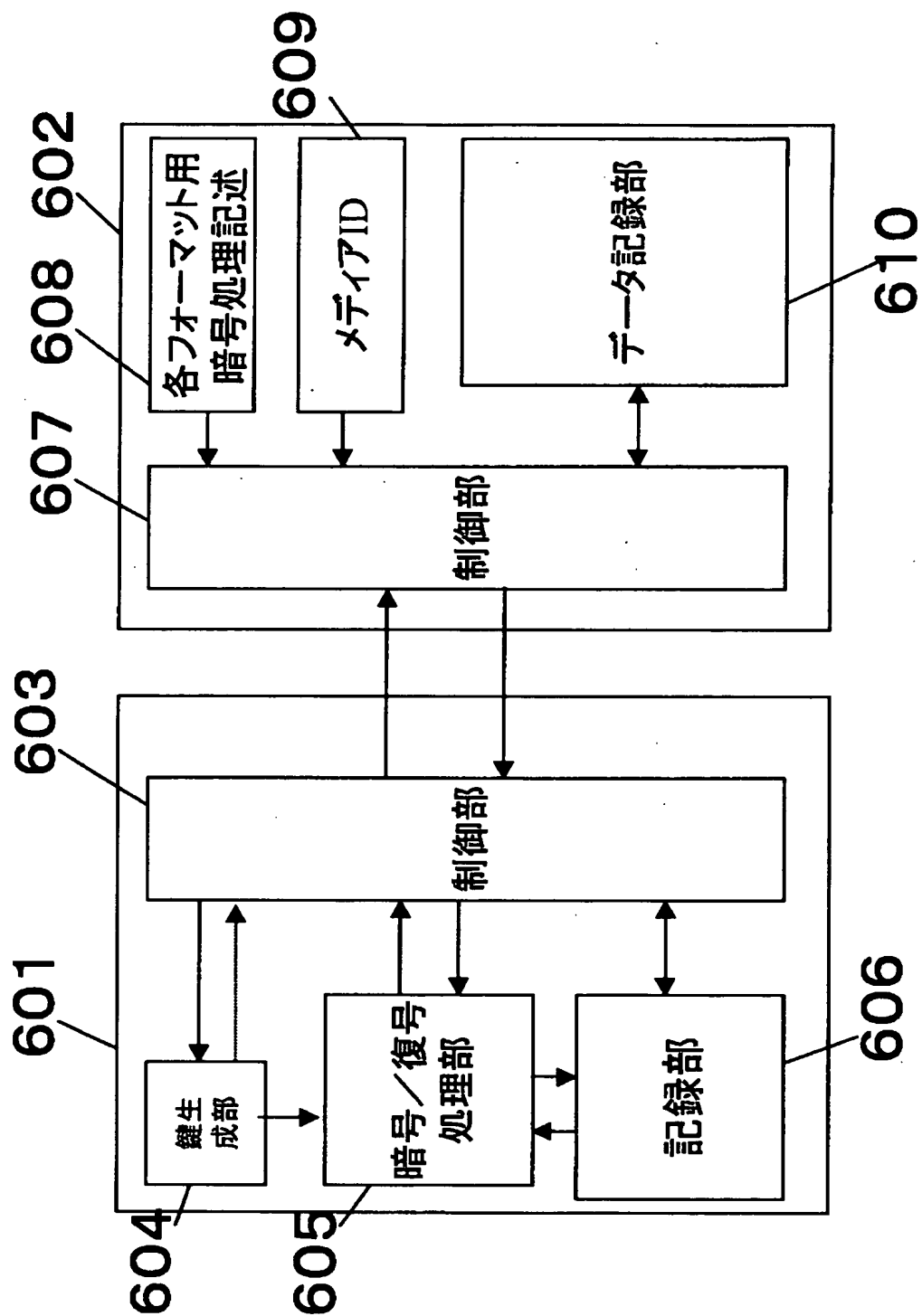
【図 4】



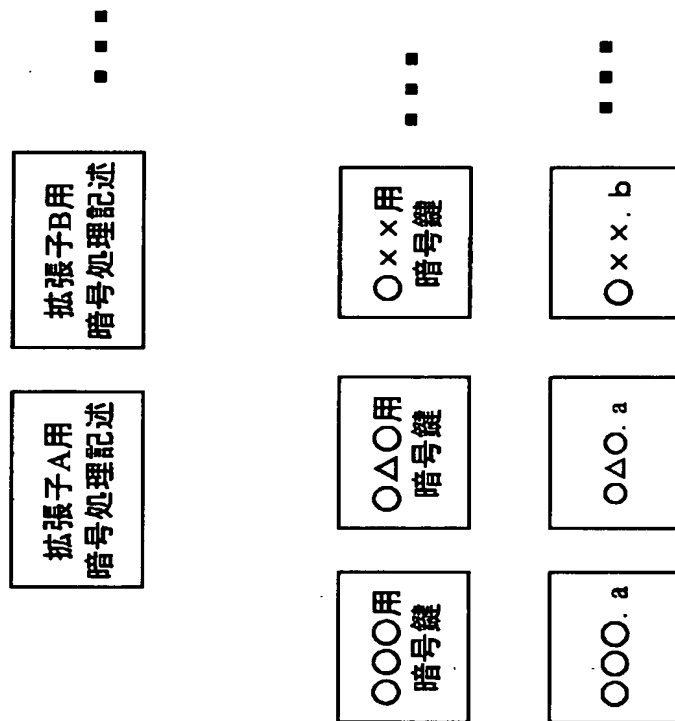
【図 5】



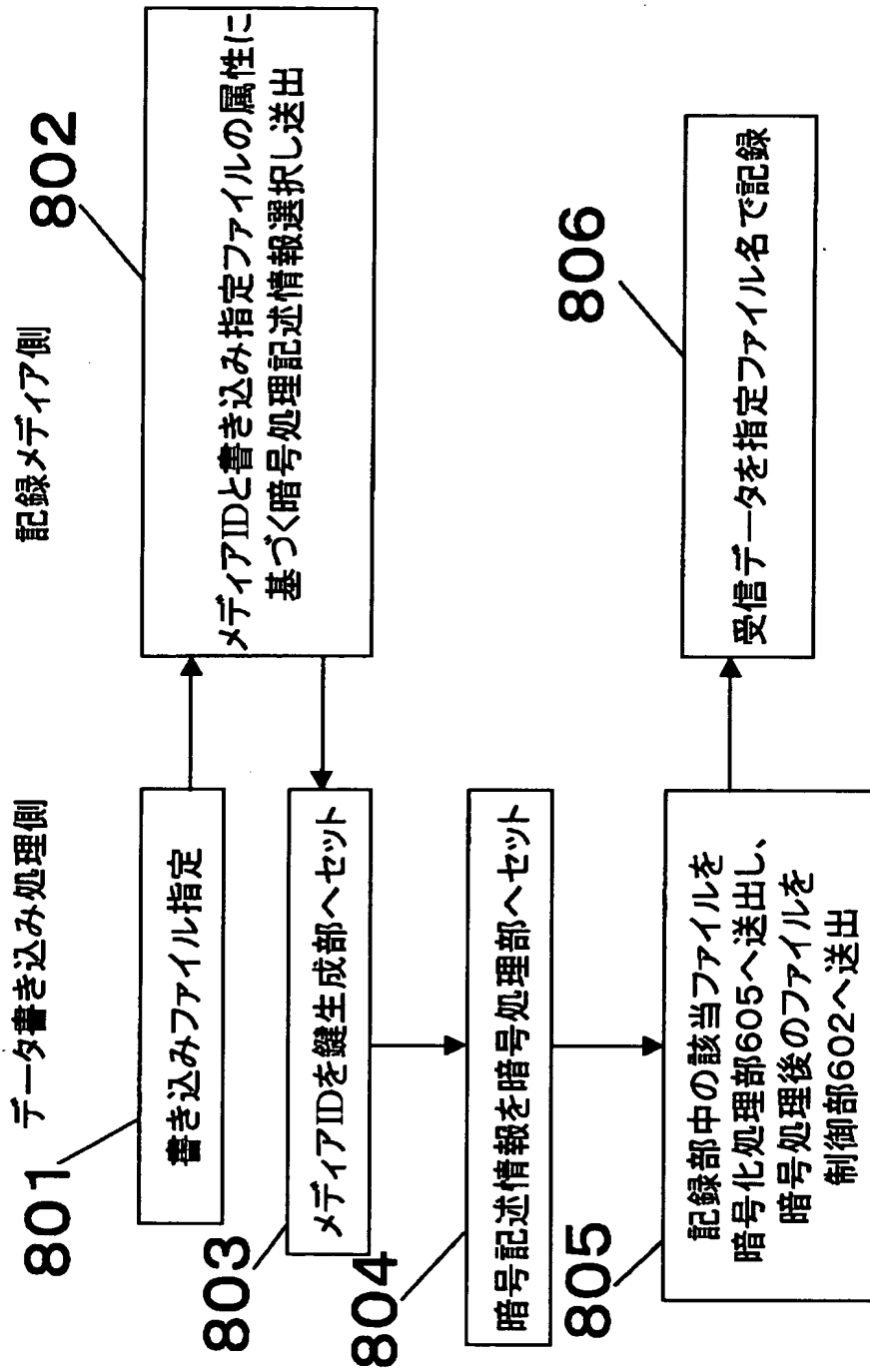
【図 6】



【図 7】

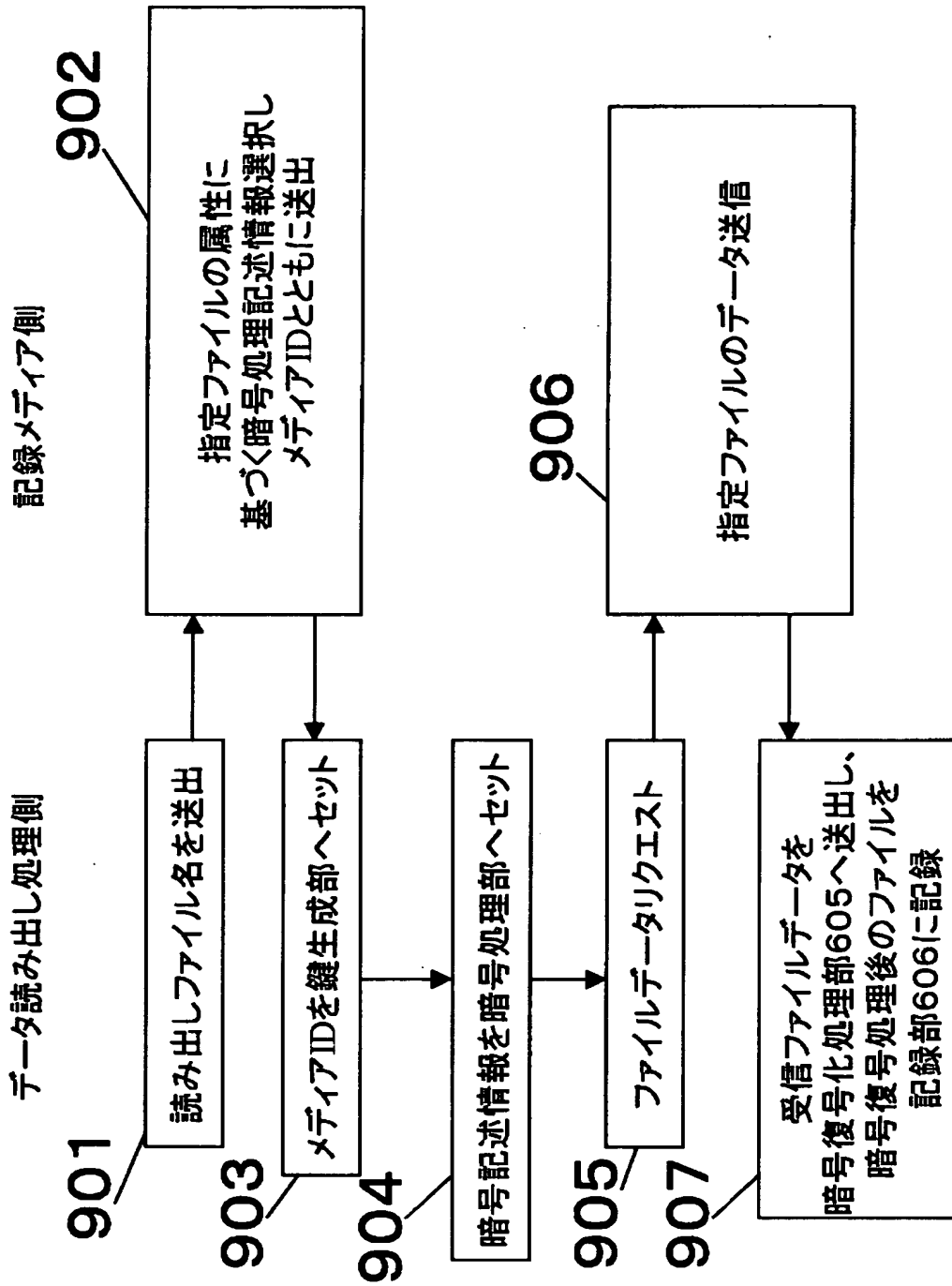


【図 8】

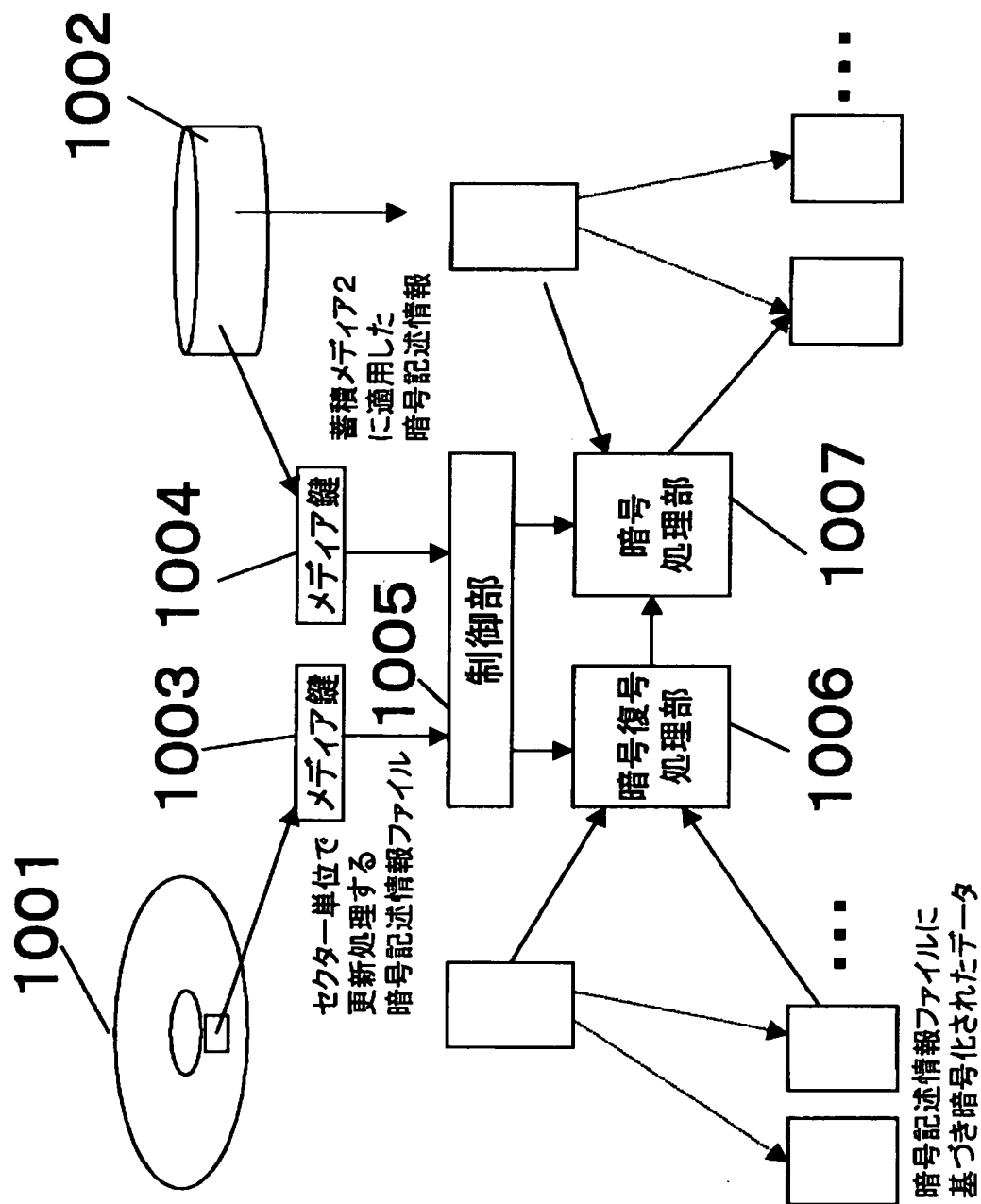




【図 9】



【图 10】



【図 1 1】

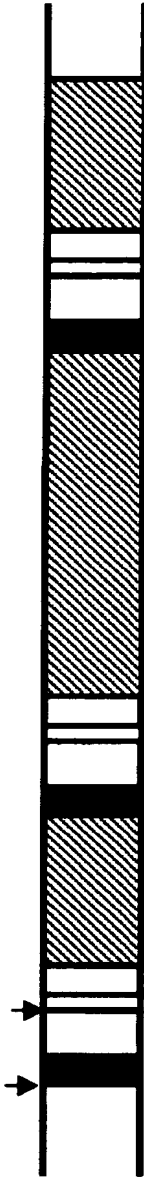
固定長でペイロードのみ暗号(ヘッダー検出必要)

同期パターン



可変長ペイロードのみ暗号(ヘッダーおよびフレーム長検出必要)

同期パターン フレーム長コード



固定長で一定周期毎に処理更新(更新周期の指定)



【書類名】 要約書

【要約】

【課題】 多様なデジタルデータについて、そのフォーマットに適した暗号化処理位置に暗号化処理を行う暗号化処理装置を提供することを目的とする。

【解決手段】 制御部 1 0 2 は、暗号処理記述情報に基づき、ヘッダー検出部 1 0 5 およびフレーム長検出部 1 0 4 を制御して入力データ中の暗号処理領域を求め、その暗号領域に暗号化処理するように暗号処理部 1 0 3 を制御する。入力データに応じて暗号処理記述情報を書き換えることにより、入力データに適した暗号化処理を行える。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [ 0 0 0 0 0 5 8 2 1 ]

1. 変更年月日	1 9 9 0 年 8 月 2 8 日
[変更理由]	新規登録
住 所	大阪府門真市大字門真 1 0 0 6 番地
氏 名	松下電器産業株式会社